## AMENDMENTS TO THE CLAIMS

1. (Currently amended) In a computer system comprising a plurality of nodes interconnected for communication via a network, a method including acts of:

(A) capturing, in a first data structure of a plurality of data structures, a notification provided by a node on the network, the notification having a characteristic and comprising at least a portion of a transmission by the node, the transmission describing a network event, the first data structure being selected among the plurality of data structures to store the notification based at least in part on the characteristic;

(B) identifying a data element within the notification;

(C) updating an index, based on the data element, with an indication of a location within the first data structure where the data element is recorded;

wherein the data element identifies a notification type for the notification, an originating internet protocol (IP) address for the notification and/or a destination IP address for the notification; and

wherein the characteristic comprises an IP address of the node and/or a time period during which the notification occurred.

2. (Currently amended) The method of claim 1, wherein the act (A) further comprises storing the first data structure in a non-volatile storage.

3. (Currently amended) The method of claim 2, wherein the act (A) further comprises storing the first data structure in a file system in the non-volatile storage.

4. (Original) The method of claim 3, wherein the file system is a hierarchical file system.

5-6. (Canceled).

7. (Currently amended) The method of claim 1, wherein the first data structure is a file.

8. (Currently amended) The method of claim 2, further comprising an act of compressing the first data structure.

9. (Currently amended) The method of claim 2, further comprising an act of creating a digital signature for the first data structure.

10. (Original) The method of claim 1, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

11. (Currently amended) The method of claim 1, further comprising acts of:

(D) accessing the index to determine, based on the indication, the location of the data element within the first data structure; and

(E) accessing the data element at the location.

12. (Original) The method of claim 1, further comprising an act of creating a summary based at least in part on a presence of the data element within the notification.

13. (Original) The method of claim 12, further comprising an act comprising accessing the summary to determine the presence of the data element within the first data structure.

14. (Currently amended) At least one computer-readable medium encoded with instructions which, when executed by a computer, perform a method in a computer system comprising a plurality of nodes interconnected for communication via a network, a method including acts of:

(A) capturing, in a first data structure of a plurality of data structures, a notification provided by a node on the network, the notification having a characteristic and comprising at least a portion of a transmission by the node, the transmission describing a network event, the first data structure being selected among the plurality of data structures to store the notification based at least in part on the characteristic;

(B) identifying a data element within the notification;

(C) updating an index, based on the data element, with an indication of a location within the first data structure where the data element is recorded;

wherein the data element identifies a notification type for the notification, an originating internet protocol (IP) address for the notification and/or a destination IP address for the notification; and

wherein the characteristic comprises an IP address of the node and/or a time period during which the notification occurred.

15. (Currently amended) The at least one computer-readable medium of claim 14, further comprising instructions defining storing the first data structure in a non-volatile storage.

16. (Currently amended) The at least one computer-readable medium of claim 15, further comprising instructions defining storing the first data structure in a file system in the non-volatile storage.

17. (Original) The at least one computer-readable medium of claim 16, wherein the file system is a hierarchical file system.

18-19. (Canceled).

20. (Currently amended) The at least one computer-readable medium of claim 14, wherein the first data structure is a file.

21. (Currently amended) The at least one computer-readable medium of claim 15, further comprising instructions defining compressing the first data structure.

22. (Currently amended) The at least one computer-readable medium of claim 15, further comprising instructions defining creating a digital signature for the first data structure.

23. (Original) The at least one computer-readable medium of claim 14, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

24. (Currently amended) The at least one computer-readable medium of claim 14, further comprising instructions defining accessing the index to determine, based on the indication, the location of the data element within the first data structure; and accessing the data element at the location.

25. (Original) The at least one computer-readable medium of claim 14, further comprising instructions defining creating a summary based at least in part on a presence of the data element within the notification.

26. (Currently amended) The at least one computer-readable medium of claim 25, further comprising instructions defining accessing the summary to determine the presence of the data element within the first data structure.

27. (Currently amended) A system for monitoring activity occurring in a computer system comprising a plurality of nodes interconnected for communication via a network, the system comprising at least one processor programmed to implement:

a capture controller, said capture controller capturing, in a first data structure of a plurality of data structures, a notification provided by a node on the network, the notification having a characteristic and comprising at least a portion of a transmission by the node, the transmission describing a network event, the first data structure being selected among the plurality of data structures to store the notification based at least in part on the characteristic;

an identification controller, said identification controller identifying a data element within the notification;

an update controller, said update controller updating an index, based on the data element, with an indication of a location within the first data structure where the data element is recorded;

wherein the data element identifies a notification type for the notification, an originating internet protocol (IP) address for the notification and/or a destination IP address for the notification; and

wherein the characteristic comprises an IP address of the node and/or a time period during which the notification occurred.

28. (Currently amended) The system of claim 27, wherein the capture controller further stores the first data structure in a non-volatile storage.

29. (Currently amended) The system of claim 28, wherein the capture controller further stores the first data structure in a file system in the non-volatile storage.

30. (Original) The system of claim 29, wherein the file system is a hierarchical file system.

31-32. (Canceled).

33. (Currently amended) The system of claim 27, wherein the first data structure is a file.

34. (Currently amended) The system of claim 28, further comprising a compression controller, said compression controller compressing the first data structure.

35. (Currently amended) The system of claim 28, further comprising a signature controller, said signature controller creating a digital signature for the first data structure.

36. (Original) The system of claim 27, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

37. (Currently amended) The system of claim 27, further comprising:

an access controller, said access controller accessing the index to determine, based on the indication, the location of the data element within the first data structure; and accessing the data element at the location.

38. (Original) The system of claim 27, further comprising a summary controller, said summary controller creating a summary based at least in part on a presence of the data element within the notification.

39. (Currently amended) The system of claim 38, further comprising a summary access controller, said summary access controller accessing the summary to determine the presence of the data element within the first data structure.

40-81. (Canceled).

82. (Currently amended) A system for monitoring activity occurring in a computer system comprising a plurality of nodes interconnected for communication via a network, the system comprising at least one processor programmed to implement:

means for capturing, in a first data structure of a plurality of data structures, a notification provided by a node on the network, the notification having a characteristic and comprising at least a portion of a transmission by the node, the transmission describing a network event, the first data structure being selected among the plurality of data structures to store the notification based at least in part on the characteristic;

means for identifying a data element within the notification;

means for updating an index, based on the data element, with an indication of a location within the first data structure where the data element is recorded;

wherein the data element identifies a notification type for the notification, an originating internet protocol (IP) address for the notification and/or a destination IP address for the notification; and

wherein the characteristic comprises an IP address of the node and/or a time period during which the notification occurred.

83. (Currently amended) The system of claim 82, wherein the means for capturing stores the first data structure in a non-volatile storage.

84. (Currently amended) The system of claim 83, wherein the means for capturing stores the first data structure in a file system in the non-volatile storage.

85. (Original) The system of claim 84, wherein the file system is a hierarchical file system.

86-87. (Canceled).

88. (Currently amended) The system of claim 82, wherein the first data structure is a file.

89. (Currently amended) The system of claim 83, further comprising means for compressing the first data structure.

90. (Currently amended) The system of claim 83, further comprising means for creating a digital signature for the first data structure.

91. (Original) The system of claim 82, wherein the transmission comprises at least one of a SYSLOG message, an SNMP message, a NetFlow message and a TCP packet.

92. (Currently amended) The system of claim 82, further comprising:

means for accessing the index to determine, based on the indication, the location of the data element within the first data structure; and

means for accessing the data element at the location.

93. (Original) The system of claim 82, further comprising means for creating a summary based at least in part on a presence of the data element within the notification.

94. (Currently amended) The system of claim 93, further comprising means for accessing the summary to determine the presence of the data element within the first data structure.

95-108. (Canceled).

109. (New) The method of claim 1, wherein the data element identifies a notification type for the notification.

110. (New) The method of claim 1, wherein the data element identifies an originating internet protocol (IP) address for the notification.

111. (New) The method of claim 1, wherein the data element identifies a destination IP address for the notification.

112. (New) The method of claim 1, wherein the characteristic comprises an IP address of the node.

113. (New) The method of claim 1, wherein the characteristic comprises a time period during which the notification occurred.

114. (New) The at least one computer-readable medium of claim 14, wherein the data element identifies a notification type for the notification.

115. (New) The at least one computer-readable medium of claim 14, wherein the data element identifies an originating internet protocol (IP) address for the notification.

116. (New) The at least one computer-readable medium of claim 14, wherein the data element identifies a destination IP address for the notification.

117. (New) The at least one computer-readable medium of claim 14, wherein the characteristic comprises an IP address of the node.

118. (New) The at least one computer-readable medium of claim 14, wherein the characteristic comprises a time period during which the notification occurred.

119. (New) The system of claim 27, wherein the data element identifies a notification type for the notification.

120. (New) The system of claim 27, wherein the data element identifies an originating internet protocol (IP) address for the notification.

121. (New) The system of claim 27, wherein the data element identifies a destination IP address for the notification.

122. (New) The system of claim 27, wherein the characteristic comprises an IP address of the node.

123. (New) The system of claim 27, wherein the characteristic comprises a time period during which the notification occurred.

124. (New) The system of claim 82, wherein the data element identifies a notification type for the notification.

125. (New) The system of claim 82, wherein the data element identifies an originating internet protocol (IP) address for the notification.

126. (New) The system of claim 82, wherein the data element identifies a destination IP address for the notification.

127. (New) The system of claim 82, wherein the characteristic comprises an IP address of the node.

128. (New) The system of claim 82, wherein the characteristic comprises a time period during which the notification occurred.